UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/803,210	03/08/2001	Janez Skubic	34650-00679USPT	8563

7590 09/28/2004

JENKENS & GILCHRIST, P.C.
1445 Ross Avenue, Suite 3200
Dallas, TX 75202-2799

EXAMINER	
GIANOLA, JOHN F	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/803,210	SKUBIC ET AL.	
	Examiner	Art Unit	
	John F Gianola	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03-08-2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 2, 4-6, 8-11, 13-16, 30, and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Ynjiun Wang (US Pat. No. 5,917,913).

3. Referring to Claim 1:

Wang discloses:

receiving the document to be digitally signed at a first location (see Figure 2 and column 4, lines 12-20 and lines 40-42);

generating a representation of the document (see Figure 7 and column 4, lines 22-25 and lines 40-41);

forwarding the representation of the document to a personal trusted device (see column 4, lines 9-16 and lines 40-44); and

digitally signing the representation of the document at the personal trusted device (see column 12, lines 65-66).

4. With respect to Claim 2:

Wang discloses the limitations of Claim 1, as well as:

wherein the first location comprises a trusted PC (see column 4, lines 16-20).

With regards to Claim 4:

Wang discloses the limitations of Claim 2, as well as:

Entering a PIN into the personal trusted device (see column 11, lines 5-10).

5. With respect to Claim 5:

Wang discloses the limitations of Claim 2, as well as:

wherein the step of forwarding further comprises the steps of establishing a serial cable connection between the personal trusted device and the trusted PC (see column 4, lines 33-39).

6. With respect to Claim 6:

Wang discloses the limitations of Claim 2, as well as:

wherein the step of forwarding further comprises the steps of establishing a infrared connection between the personal trusted device and the trusted PC (see column 4, lines 30-31).

7. With regards to Claim 8:

Wang discloses the limitations of Claim 2, as well as:

displaying the document at the trusted PC prior to digitally signing the representation (see column 4, lines 40-43).

8. With regards to Claim 9:

Wang discloses the use of encryption to secure communications between a first location and a device (see column 5, lines 1-18). Because data sent from the first location to the device is encrypted, it is inherent that the first location contains a cryptography module. Thus, Wang discloses:

wherein the first location comprises a cryptography module within a PC.

9. With regards to Claim 10:

Wang discloses the limitations of Claim 9 above as well as displaying a document on a computer terminal in a network (see column 4, lines 16-18). Based upon the definition of a browser—software that translates digital bits into pictures and text—it is inherent that Wang's teaching discloses:

Displaying the document at the PC in a browser associated with the cryptography module (see the entry for "browser" in Newton, Harry. *Newton's Telecom Dictionary.* New York: CMP Books, 2002).

10. With respect to Claim 11:

Wang discloses the limitations of Claim 1 above, as well as:

Forwarding the document from the first location to a trusted third party (see Figure 2 and column 4, lines 13-27).

11. With respect to Claim 13:

Wang discloses the limitations of Claim 1 above, as well as:

Forwarding the document to a server prior to generation of the representation of the document (Figure 2 and column 4, lines 16-20);

Forwarding the document and the representation of the document from the server to the trusted party (see column 4, lines 13-16 and lines 22-25 and column 13, lines 1-2).

12. With respect to Claim 14:

Wang discloses the limitations of Claim 1 above, as well as:

Streaming the representation and at least a portion of the document to the personal trusted device (see column 12, line 65 to column 13, line 2; and column 11, lines 54-57).

13. With regards to Claim 15:

Wang discloses the limitations of Claim 14 above, as well as:

Selecting portions of the document to be streamed to the personal trusted device (see column 4, lines 22-25); and

Displaying the selected portions at the personal trusted device (see column 4, lines 40-43).

14. With respect to Claim 16:

Wang discloses the limitations of Claim 14 above, as well as:

Displaying only portions of the document contained within a buffer of the personal trusted device (see Figure 6B; column 4, lines 22-25; and column 11, lines 17-27).

15. With regards to Claim 30:

Wang discloses:

Receiving the document to be digitally signed at a personal computer (see column 4, lines 16-20);

Generating a hash from the document at the personal computer (see Figure 7 and column 4, lines 22-25 and lines 40-41);

Streaming the hash and at least of portion of the document to a mobile terminal (see column 4, lines 9-16 and lines 40-44); and

Digitally signing the hash at the mobile terminal (see column 12, lines 65-66).

16. With respect to Claim 33:

Wang discloses

A personal computer for receiving the document to be digitally signed and enabling generation of a hash of the document (see column 4, lines 16-18;); and

A personal trusted device for displaying the hash and for enabling digital signing of the hash (see column 4, lines 40-44; column 12, lines 65-67).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

19. Claim 3 rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier (Schneir, Bruce. *Applied Cryptography.* New York: Wiley and Sons, 1996). Wang discloses using encryption, specifically public key encryption, to secure communications between a first location and a device (see Wang: column 4, line 66 to

column 5, line 3; and column 5, lines 37-50). Wang, however, does not specifically mention:

Including the step authenticating an identity of the trusted PC by the personal trusted device.

Schneier teaches the use of public key cryptography to authenticate identities (see Schneier: pages 53 and 54). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wang's invention with Schneier's teaching in order to increase the security of the communications between the first location and the device (see page 24 of Menezes et. al. *Handbook of Applied Cryptography.* New York: CRC Press, 1997).

20. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Mettala et. al. (Mettala et. al. "Bluetooth Protocol Architecture Version 1.0" Bluetooth Special Interest Group, 8 August 1999). Wang teaches communication between the first location and the device using wireless communication (see Wang: column 4, lines 31-33). Wang fails to specifically teach a wireless protocol for this communication. The Bluetooth Protocol is a standard wireless protocol. It would have obvious to one of ordinary skill in the art at the time of the invention to combine Wang's teaching with the Bluetooth Standard in order to allow for the development of interoperable applications (see Mettala et. al.: page 16).

21. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Dierks et. al. (Dierks, T. and C. Allen. *The TLS Protocol Version 1.0.* Internet Engineering Task Force, 1999. Request for Comment #2246). While Wang teaches the use of Public-Key and symmetric key encryption algorithms for security (see Wang, column 5, lines 37-50), he fails to specifically teach the SSL/TSL protocol. However, Dierks et. al. teach the SSL/TLS protocol as a means for using encryption to secure communications (see Dierks et. al.: "Section 1. Introduction"). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wang's teaching with the TLS standard in order to have security that is application protocol independent (see Dierks et. al.: "Section 1. Introduction").

22. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang discloses the limitations of Claim 1 above, as well as:

Forwarding the document to the personal trusted device (see Wang: column 4, lines 14-16);

Generating a second representation of the document at the personal trusted device (see Wang: column 4, lines 44-47 and column 7, lines 1-12). Wang fails to specifically mention comparing the first and second representation. Wang does, however, mention using public-key encryption (as well as other algorithms and protocols) and signing documents. Schneier specifically teaches the use of public-key encryption and one-way hash functions to generate a first and second representation and compare the two (see Schneier: page 38). It would have been obvious to one of

ordinary skill in the art at the time of the invention to combine Wang's device with Schneier's teaching in order to increase the security of device.

23. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang discloses:

Receiving the document to be digitally signed at a personal computer (see Wang: column 4, lines 16-20);

Generating a hash from the document at the personal computer (see Wang: Figure 7 and column 4, lines 22-25 and lines 40-41);

Forwarding the hash to the mobile terminal (see Wang: column 4, lines 12-20 and lines 40-42); and

Displaying the document at the personal computer (see Wang: column 4, lines 40-43);

Displaying the hash at the mobile terminal (see Wang: column 4, lines 40-43); and

Digitally signing the hash of the document at the mobile terminal (see Wang: column 12, lines 65-66). Wang discuses the use of public-key encryption to secure the communications between the personal computer and mobile terminal, but does not specifically teach the mobile terminal authenticating the personal computer. Schneier teaches the use of public-key encryption to authenticate identities in order to increase security (see Schneier: pages 53 and 54). It would have obvious to one of ordinary skill

in the art at the time of the invention to combine Schneier's teachings of authentication with Wang's invention in order to increase security between the two devices.

24. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang and Schneier disclose the limitations of Claim 18 as noted above and Wang further discloses:

The step of entering a PIN into the mobile terminal (see Wang: column 11, lines 5-10).

25. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang and Schneier disclose the limitations of Claim 18 as noted above and Wang further discloses:

Establishing a serial cable connection between the mobile terminal and the personal computer (see Wang: column 4, lines 33-39).

26. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang and Schneier disclose the limitations of Claim 18 as noted above and Wang further discloses:

Establishing an infrared connection between the mobile terminal and the personal computer (see Wang: column 4, lines 30-31).

27. Claim 22 rejected under 35 U.S.C. 103(a) as being unpatentable over Wang and Schneier as applied to Claim 18 above, and further in view of Mettala et. al. Wang and Scheier disclose the limitations of Claim 18 as noted above, as well as establishing communications using wireless connections, but fail to specifically teach establishing a Bluetooth connection. The Bluetooth Protocol is an industry standard wireless protocol. It would have obvious to one of ordinary skill in the art at the time of the invention to combine Wang's teaching with the Bluetooth Standard in order to allow for the development of interoperable applications (see Mettala et. al.: page 16).

28. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang and Schneier. Wang and Schneier disclose the limitations of Claim 18 as noted above. Wang further discloses displaying a document on a computer terminal in a network (see Wang: column 4, lines 16-20). Based upon the definition of a browser—software that translates digital bits into pictures and text—it is inherent that Wang's teaching discloses:

Displaying the document in a browser at the personal computer.

29. Claim 24 rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang and Schneier disclose the limitations of claim 18 as referenced above, and Wang further discloses:

Wherein the personal computer comprises a trusted personal computer (see Wang: column 4, lines 16-20).

30. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang and Schneier disclose the limitations of Claim 18 as noted above. Wang further discloses the use of encryption to secure communications between a first location and a device (see Wang: column 5, lines 1-18). Because the transaction data sent from the first location to the device is encrypted, it is inherent that the first location contains a cryptography module for encrypting data, which includes the creation of hashes. Thus, Wang discloses:

Generating the hash from the document at a cryptography module in the personal computer.

31. Claim 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Schneier. Wang and Schneier disclose the limitations of Claim 18 as noted above, and Wang further discloses:

Forwarding the document to the personal trusted device (see Wang: column 4, lines 12-20 and lines 40-42);

Generating a second hash of the document at the personal trusted device (see Wang: column 4, lines 44-47 and column 7, lines 1-12). However, Wang fails to specifically mention comparing the first and second representation. Wang discloses the use of public-key encryption (as well as other algorithms and protocols) and the signing of documents. Schneier specifically teaches the use of public-key encryption and one-way hash functions to generate a first and second representation and compare the two

(see Schneier: page 38). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Wang's device with Schneier's teaching in order to increase the security of device.

32. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal (US Pat. No. 5,671,279) in view of Wang. Elgamal discloses electronic commerce using digital signatures, but not the use of a personal trusted device. Wang discloses a personal trusted device for digitally signing documents in an electronic transaction system. Elgamal discloses:

Receiving the document to be digitally signed at a personal computer (see Elgamal: column 6, lines 30-36 and column 9, lines 55-60);

Forwarding the document to a server (see Elgamal: column 9, lines 61-63);

Generating a hash from the document at the server (see Elgamal: column 9, lines 12-13);

Forwarding the hash and the document from the server to a trusted third party from the server (see Elgamal: column 13, lines 26-29).

Elgamal then teaches forwarding the hash to a client, but not the use of a mobile terminal (see Elgamal: column 11, lines 46-47; Elgamal column 7, lines 37-38). However, Wang discloses receiving and signing the hash of a forwarded document on a mobile terminal (see Wang: column 4, lines 10-30). Thus the combination of Elgamal and Wang disclose:

Forwarding the hash to a mobile terminal from the trusted third party; and

Digitally signing the hash of the document at the mobile terminal.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use Wang's device in conjunction with Elgamal's electronic transaction system in order to substantially eliminate the risk of unauthorized access to the user's account (see Wang: column 2, lines 56-60).

33. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Wang. Elgamal and Wang disclose the limitations of Claim 27 above. Elgamal also discloses:

Forwarding the documents using SSL/TLS protocol (see Elgamal: column 9, lines 4-7).

34. Claim 29 rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Wang. Elgamal and Wang disclose the limitations of Claim 27 as referenced above, and Elgamal further discloses:

Requesting a digital signature at the PC (see Elgamal: column 13, lines 6-19).

35. With respect to Claim 31:

Elgamal and Wang disclose the limitations of Claim 28 as noted above, Wang further discloses:

The personal computer further displays the document (see Wang: column 4, lines 40-43);

36. With respect to Claim 32:

Elgamal and Wang disclose the limitations of Claim 28 as noted above. Wang also discloses viewing the document at a mobile terminal (see Wang: column 4, lines 40-44). Thus it is inherent that Wang discloses:

Displaying only portions of the document contained with a buffer of the mobile terminal.

37. With regards to Claim 34:

Elgamal and Wang disclose the limitations of Claim 31 above and Wang further discloses:

The personal computer further displays the document (see Wang: column 4, lines 40-44).

38. With respect to Claim 35:

Elgamal and Wang disclose the limitations of Claim 31 above and Wang teaches the use of encryption to secure communications between a first location and a device (see Wang: column 5, lines 1-18). Because data sent from the first location to the device is encrypted, it is inherent that the first location contains a cryptography module. Thus, Wang discloses:

A cryptographic module for enabling generation of the hash.

39. With regards to Claim 36:

Elgamal and Wang disclose the limitations of Claim 31 as noted above, Wang further discloses:

A server for generating the hash from the document; and

A trusted party for providing the hash to the personal trusted device (see Wang: Figure 2 and Wang: column 4, lines 16-20).

40. With respect to Claim 37:

Elgamal and Wang disclose the limitations of Claim 31 as noted above, Wang further discloses:

Wherein the personal computer streams the hash and at least a portion of the document to the mobile terminal (see Wang: column 12, line 65 to column 13, line 2 and Wang: column 11, lines 54-57).

Conclusion

40. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Johnson et. al. "Masked Digital Signatures" (US Pat. No. 6,279,110 B1); Vanstone "Digital Signature Protocol" (US Pat. No. 6,212,281 B1); Gennaro et. al. "Undeniable Certificates for Digital Signature Verification" (US Pat. No. 6,292,897 B1); and Cohen "Method and Apparatus for Secure Electronic Transaction Authentication" (US PGP No. US 2002/0099664 A1).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John F Gianola whose telephone number is (703) 605-4321. The examiner can normally be reached on Mon - Fri (8:30 - 5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

In October of 2004, Technology Center 2100 will be relocating to the US Patent and Trademark Office's facility in Alexandria, VA. After that date, calls to John F Gianola should be directed to (571) 272-3848. Likewise, the telephone number for Technology Center 2100 will change to (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KIM VU
SUPERVISORY PATENT EXA...
TECHNOLOGY CENTER 21...